

AMENDMENTS TO THE CLAIMS**RECEIVED
CENTRAL FAX CENTER****MAR 26 2009**

1 1. (Currently amended) An apparatus, comprising:
2 an authentication device that authenticates a computing device, in
3 communication with the authentication device, through employment of a determination
4 that a current location of the authentication device matches an initial location of the
5 authentication device;

6 wherein one or more private keys employable for encryption and/or decryption of
7 information are erased via an automatic cutoff of power upon an attempt to move the
8 authentication device.

1 2. (Previously presented) The apparatus of claim 1, wherein the computing
2 device comprises a first computing device; and

3 wherein the authentication device makes the determination that the current
4 location of the authentication device matches the initial location of the authentication
5 device in response to a request from a second computing device for authentication of
6 the first computing device for a data transfer from the second computing device to the
7 first computing device.

1 3. (Previously presented) The apparatus of claim 2, wherein the request from
2 the second computing device comprises an authentication challenge string; and

3 wherein the authentication device stores the one or more private keys, and
4 wherein if the current location of the authentication device matches the initial location of
5 the authentication device, then the authentication device employs one or more of the
6 one or more private keys to decrypt the authentication challenge string into an
7 authentication challenge response.

1 4. (Previously presented) The apparatus of claim 3, wherein the
2 authentication device sends the authentication challenge response to the second
3 computing device, and wherein the second computing device analyzes the
4 authentication challenge response to determine whether the first computing device is
5 authenticated for the data transfer.

1 5. (Previously presented) The apparatus of claim 4, wherein the second
2 computing device comprises an authentication challenge key to compare with the
3 authentication challenge response received from the authentication device; and

4 wherein if the authentication challenge response matches the authentication
5 challenge key, then the authentication challenge response represents that the first
6 computing device is authenticated and the data transfer can be sent from the second
7 computing device to the first computing device.

1 6. (Original) The apparatus of claim 3, wherein upon determination that the
2 current location of the authentication device does not match the initial location of the
3 authentication device, the authentication device prevents authentication of the first
4 computing device and disables the one or more private keys.

1 7. (Previously presented) The apparatus of claim 6, wherein the
2 authentication device stores the one or more private keys in volatile memory, and
3 wherein upon determination that the current location of the authentication device does
4 not match the initial location of the authentication device, the authentication device cuts
5 off power to the volatile memory to erase the one or more private keys.

1 8. (Previously presented) The apparatus of claim 1, wherein the
2 authentication device comprises a base portion, a cover portion, and one or more
3 electronic components that serve to authenticate the computing device; and
4 wherein the base portion is fixed to a surface near the computing device, and
5 wherein the cover portion is fixed to the base portion to provide a secure shell for the
6 one or more electronic components.

1 9. (Previously presented) The apparatus of claim 8, wherein a first one of the
2 base and cover portions receives electricity through a power port, and wherein a second
3 one of the base and cover portions receives electricity through an electrical contact with
4 the first one of the base and cover portions; and
5 wherein upon separation of the second one of the base and cover portions from
6 the first one of the base and cover portions, the second one of the base and cover
7 portions loses power and prevents authentication of the computing device.

1 10. (Previously presented) The apparatus of claim 9, wherein the second one
2 of the base and cover portions electrically supports one or more of the one or more
3 electronic components that store the one or more private keys, and wherein the
4 authentication device employs one or more of the one or more private keys to
5 authenticate the computing device; and

6 wherein a loss of power in the second one of the base and cover portions erases
7 the one or more private keys from the one or more of the one or more electronic
8 components.

1 11. (Previously presented) The apparatus of claim 1, wherein the
2 authentication device comprises a location sensor; and

3 wherein upon initialization of the authentication device, the location sensor sets
4 the initial location of the authentication device; and

5 wherein the location sensor determines the current location of the authentication
6 device, and wherein the authentication device compares the current location with the
7 initial location to authenticate the computing device.

1 12. (Previously presented) The apparatus of claim 11, wherein the location
2 sensor comprises a global positioning system component, and wherein the global
3 positioning system component measures the initial location and the current location of
4 the authentication device as a three-dimensional location of latitude, longitude, and
5 altitude.

- 1 13. (Original) The apparatus of claim 1, wherein the authentication device
2 allows authentication of the computing device upon the determination that the current
3 location of the authentication device matches the initial location of the authentication
4 device within a specified error range.

BEST AVAILABLE COPY